

RECEIVED
CENTRAL FAX CENTER

Appn No: 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006

DEC 0 5 2006

REMARKS/ARGUMENTS

Claims 3-5, 7-15 and 18-28 are pending in the present application of which claims 4, 10-12 and 18-26 are withdrawn.

In the Office action, claim 3 is rejected under 35 U.S.C. 103(a) over Geiger (U.S. Pat. 6,377,810) and Havinis (U.S. Pat. 6,360,102), and claims 5, 7-9, 13-15, 27 and 28 are rejected under 35 U.S.C. 103(a) over Geiger in view of Havinis and Strunk (U.S. Pub. 2002/0068551). In view of the foregoing amendments and the following remarks, Applicant believes that claims 3, 5, 7-9, 13-15, 27 and 28 are allowable.

Brief Description of Geiger and Havinis

Referring to Geiger, and in particular to FIG. 3, the mobile device 15 reports its location to the location server 21, as shown by arrow 100. A requesting entity 25 that wishes to request the location of the mobile device 15 sends a location permission request to the mobile device 15, as shown by arrow 102. The mobile device 15 then replies with a location access permission attribute certificate. The requesting entity 25 delivers the permission attribute certificate to the location server 21, as shown by arrow 105. The location server 21 validates the certificate and sends the requesting entity 25 the location of the mobile device 15. Therefore, each time a requesting entity wishes to locate a mobile device, it must directly contact the mobile device to receive permission from the mobile device. This is disclosed in column 5, lines 49-63 of Geiger as follows:

Thus, a method and system have been described by which a user of a mobile device provides permission to the requesting entity by creating and signing the attribute certificate containing a location permission attribute of the user's device for a specific time window and optionally for specific geographic regions. This attribute certificate is issued to the entity requesting the location information for which the user has decided to allow access. A location server receiving a request

**Appln No. 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006**

for location information from an entity that provides such a correctly authorized attribute certificate securely sends this information to the requesting entity. This transfer is secured by either establishment of a secure session using a key exchange mechanism to create a session key or by encrypting the information with the requesting entities public encrypting key.

According to the above-quoted portion, the objective of Geiger is to make the location information of the mobile device highly private and secure. To accomplish this, a requestor not only has to directly request permission form the mobile device every time such positioning is desired, but the permission also has to be verified by the server. Applicant would also like to point out that most of the detailed description of Geiger is devoted to the method and system for accomplishing such an objective.

Furthermore, the user of the mobile device has to grant permission to the requestor every time such a request is made by responding to the request through the mobile device. This is disclosed in column 4, lines 7-25 of Geiger as follows:

The mobile device 15 receives the location and permission request and verifies the identity certificate of the requesting entity using the certification key in the requesting entity domain. Verification is carried out by hashing the message and inputting the resulting hash output, the certified public key of the requesting entity, and the digital signature, into the verification part of the cryptographic algorithm. If the user 16 agrees with the request for location information, the user enters an input at the user input 16, which causes the mobile device 15 to generate a location access permission attribute certificate granting permission to the requestor. This certificate includes a digital signature generated by the mobile device 15 using the root key of the mobile communication system domain, that is the domain that is common between the mobile device 15 and the location server 21. The mobile device 15 sends this location access permission attribute certificate to the requesting entity 25 in the form of a location access granting data message on the return channel through the base station 11 and the gateway 22.

(Emphasis added).

**Appln No. 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006**

Referring to column 4, lines 5-27 of Havinis, a user of a mobile phone can define a Subscriber Location Privacy Profile (SLPP), which contains a list of preferred subscribers that have permission to position the mobile phone. Such a list can be stored on the Home Location Register (HLR) or the mobile device itself. However, if stored on the mobile device, the SLPP must be downloaded by the GMLC (Gateway Mobile Location Center), MLC (Mobile Switching Center) or serving MSC/VLR (Mobile Switching Center/Visitor Location Register) in order for other subscribers to be able to position the mobile device. (See FIGS. 6A and 6B and column 9, lines 39-48).

Therefore, in Havinis, the SLPP that is defined by the user of the mobile phone is stored in Home Location Register (HLR) or the mobile device itself. Another subscriber can position the mobile phone by requesting the position from the HLR or the mobile phone if the subscriber is on the SLPP.

Claim 3 is Patentable over Geiger in View of Havinis.

Claims 3 is rejected under 35 U.S.C. 103(a) over Geiger in view of Havinis. Applicant has amended claim 3 to specify storing the additional data regarding the user in the user-specific space, the additional data being related to the location of the user. Claim 3 also specifies providing the data indicative of the location of the user and the additional data regarding the user to possible requesters on the access list. In contrast, Geiger and Havinis fail to disclose or suggest storing the additional data regarding the user in the user-specific space, the additional data being related to the location of the user, and providing the data indicative of the location of the user and the additional data regarding the user to possible requesters on the access list, as specified in claim 3.

As discussed above, Geiger does not provide an access list of requesters to which location information of a user is provided. As also discussed above, Havinis provides a SLPP, which contains a list of preferred subscribers that have permission to position the mobile phone. Accordingly, Geiger and Havinis only provide the location of the user to a requestor and do not

**Appln No. 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006**

disclose that any additional information related to the location of the user is provided to the requestor. Thus, neither Geiger nor Havinis discloses or suggests storing the additional data regarding the user in the user-specific space, the additional data being related to the location of the user, and providing the data indicative of the location of the user and the additional data regarding the user to possible requesters on the access list, as specified in claim 3.

Based on the foregoing, Claim 3 is patentable over Geiger and Havinis.

Claims 5, 7-9, 13-15, 27 and 28 are Patentable over Geiger in View of Havinis and Strunk.

Claims 5, 7-9, 13-15 and 27-28 are rejected under 35 U.S.C. 103(a) over Geiger in view of Strunk and Havinis. Applicant has amended claim 5 to specify that the information stored in the user specific data space includes additional information related to the location of the individual associated with the PCD. In contrast, Geiger, Strunk and Havinis fail to disclose or suggest that the application server is further configured to store information received from and concerning an individual associated with the PCD in the user specific data space, wherein the information includes additional information related to the location of the individual associated with the PCD, as specified in claim 5.

As discussed above in relation to the rejection of claim 3, Geiger and Havinis fail to disclose or suggest that any additional information other than location information of a user is provided to a requester. Furthermore, Strunk fails to disclose or suggest that the stored information is related to the location of the individual associated with the PCD, as specified in claim 5.

Referring to FIGS. 1 and 7-20, and page 2, paragraphs [0017] and [0018], Strunk discloses storing contact information for a user on a network station. This contact information is shown in FIGS. 7-20 to be information such as address, email address, various telephone number, fax number, etc. However, Strunk does not disclose or even suggest that the stored information is related to the location of the individual associated with the PCD, as specified in claim 5. Furthermore, Strunk is directed to a method for only providing contact information

Appln No. 09/833,969

Amdt date December 5, 2006

Reply to Office action of July 5, 2006

through a directory assistance type of system. Accordingly, Strunk is neither concerned with the location of a PCD nor is capable of determining or storing any information related to the location of a PCD.

Therefore, because any one or a combination of Geiger, Havinis and Strunk fails to disclose or even suggest that the application server is further configured to store information received from and concerning an individual associated with the PCD in the user specific data space, wherein the information includes additional information related to the location of the individual associated with the PCD, as specified in claim 5, claims 5, 7-9, 13-15, 27 and 28 are patentable over Geiger, Havinis and Strunk.

Combining Geiger with Havinis Changes the Principle Operation of Geiger

Applicant submits that combining Geiger with Havinis would change the principle operation of Geiger. "If the proposed modification or combination of the prior art would change the principle of operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims *prima facie* obvious." MPEP Section 2143.01 (citing *In re Ratti*, 270 F.2d 810, 123 USPQ 349 (CCPA 1959)).

As described above regarding Geiger, a requesting entity has to directly communicate with the mobile device to receive a location permission request. The requesting entity then delivers the permission attribute certificate to the location server, which validates the certificate and sends the requesting entity the location of the mobile device. If the SLPP of Havinis is combined with Geiger as the Office action asserts, which is to say that permission is given to requestors to locate the mobile device based on whether the requester is on the SLPP, the entire operation of Geiger would change. In other words, Geiger would no longer operate as illustrated in FIG. 3 and would no longer operate by the user of the mobile device granting permission to each individual requestor, with the permission being validated by the server.

Based on the foregoing, Applicant submits that combining Havinis with Geiger as the Office action asserts would change the principle operation of Geiger. Accordingly, one of

**Appn No. 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006**

ordinary skill in the art would not have any motivation to combine Geiger with Havinis to provide a system and method according to the present application. Therefore, claims 3, 5, 7-9, 13-15, 27 and 28 are patentable over Geiger in view of Havinis.

Combining Geiger with Havinis Would Render Geiger Unsatisfactory for its Intended Purpose

Applicant submits that one of ordinary skill in the art would not have combined Geiger with Havinis in order to provide the system and method of the present application because such a combination would render Geiger unsatisfactory for its intended purpose. "If proposed modification would render the prior art invention being modified unsatisfactory for its intended purpose, then there is no suggestion or motivation to make the proposed modification." *MPEP* Section 2143.01 (citing *In re Gordon*, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984)).

As described above, a requestor of Geiger not only has to directly request permission from the mobile device every time it desires positioning of the mobile device, but also the permission has to be verified by the server. Geiger's intended purpose is to make the location information of the mobile device very private by having the user of the mobile device grant permission to a requestor through the input of the mobile device. In other words, Geiger intends to provide the mobile device with interactive control over the location information every time such information is requested.

In contrast, once a mobile user in Havinis creates the SLPP, any person on the list can obtain the location information of the mobile user without having to request permission from the user, i.e., the user does not have control over every location request. Accordingly, if the user does not update the SLPP on a regular basis, the user's location may be given to a requester even through the user no longer intended the requestor to have the location information.

**Appln No. 09/833,969
Amdt date December 5, 2006
Reply to Office action of July 5, 2006**

Therefore, one of ordinary skill in the art would not have combined Geiger with Havinis because such a combination would render Geiger unsatisfactory for its intended purpose. For this reason, claims 3, 5, 7-9, 13-15, 27 and 28 are patentable over Geiger in view of Havinis.

For the foregoing reasons, Applicant believes that claims 3, 5, 7-9, 13-15, 27 and 28 are allowable.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By

Saeid Mirsafian
Reg. No. 52,035
626/795-9900

SM/kmg
SM IRV1100462.2--12/5/06 5:47 PM